We claim:

1. A system for securing input of non-PIN data using a numeric keypad of a PINpad terminal, comprising:

a dynamic prompt table file arranged to permit numeric keys on the keypad to be used for entry of non-PIN data if and only if an appropriate prompt has been, and continues to be, displayed at the time of data entry; and

a file authentication arrangement for authenticating said dynamic prompt table file upon loading of the dynamic prompt table file in the terminal.

2. A system as claimed in claim 1, wherein said file authentication arrangement includes a private key and a corresponding public key certificate containing information necessary to authenticate the prompt table file.

3. A system as claimed in claim 2, wherein said private key is stored on a smartcard and is only accessible by a secure processor embedded in the smartcard.

4. A system as claimed in claim 2, further comprising a file signing tool for digitally signing said clear file, said file signing too including a smartcard reader, and wherein all digital signing operations

requiring access to said private key are carried out by a secure processor embedded in a smartcard inserted into said smartcard reader.

5. A system as claimed in claim 2, wherein said smartcard further has stored thereon a signer certificate for authenticating said digital signature, said signer certificate being authenticated by a sponsor certificate pre-installed in the terminal.

6. A method of securing input of non-PIN data using a numeric keypad of a PINpad terminal, comprising the steps of:

providing a dynamic prompt table file arranged to permit numeric keys on the keypad to be used for entry of non-PIN data if and only if an appropriate prompt has been, and continues to be, displayed at the time of data entry; and

authenticating said dynamic prompt table file upon loading of the dynamic prompt table file into the terminal.

7. A method as claimed in claim 6, wherein said authenticating step comprises the step of digitally signing the prompt table file using a private key, and appending to the signed prompt table file a corresponding public key certificate containing

information necessary to authenticate the prompt table file.

8. A system as claimed in claim 7, further comprising the steps of storing said private key on a smartcard and only permitting a secure processor embedded in the smartcard to access the private key.

9. A system as claimed in claim 8, wherein all digital signing operations requiring access to said private key are carried out by said secure processor.

10. A system as claimed in claim 7, wherein said smartcard further has stored thereon a signer certificate for authenticating said digital signature, said signer certificate being authenticated by a sponsor certificate pre-installed in the terminal.